Fernando Gómez Avilés-Casco*

LA SEGURIDAD EN LAS TRANSACCIONES

Con frecuencia se menciona la percepción de falta de seguridad de las transacciones electrónicas por parte de los usuarios como una de las principales barreras para el desarrollo del comercio electrónico. En rigor, al identificar la falta de confianza en el comercio electrónico como concepto más amplio que engloba a la presunción de falta de seguridad, es posible diseñar un conjunto de acciones que contribuyan en varios frentes a crear las condiciones de su desarrollo. Las cámaras de comercio, a nivel internacional y específicamente en España, están contribuyendo con varias iniciativas a suavizar los reparos que hacen dudar a los usuarios. La propia capilaridad de la red cameral permite contribuir en los aspectos formativos al despliegue del conocimiento y de la formación que faciliten las transacciones seguras, especialmente en el ámbito empresarial.

Palabras clave: *tecnología de la información, nuevas tecnologías, Internet, España.*
Clasificación JEL: *L86, O3.*

1. Situación actual

Frecuentemente, los estudios que analizan el comportamiento de los particulares acerca del uso de Internet destacan el incremento interanual de internautas (personas que acceden a Internet desde hace algún tiempo) y estudian el comportamiento de los internautas en relación al conjunto de la población. Dentro de los internautas estudian el caso especial de los que compran por Internet, así como las causas de que no lo haga el resto. Uno de estos estudios es el denominado *Estudio comercio electrónico B2C en España* centrado en las ventas al consumidor - B2C y elaborado por AECE-fecemd en mayo de 2003 [4].

Los datos que arroja el estudio son muy interesantes: sólo el 37,8 por 100 de los entrevistados declara utilizar Internet, por lo que éstos serán posteriormente la base sobre la que se elaboren otras conclusiones. Así y todo el incremento es notable puesto que el año anterior este porcentaje se reducía al 23,1 por 100.

Al preguntarles si compran por Internet, los internautas han respondido que sí en un 19,4 por 100 y que no en un 80,3 por 100. Por ello la representatividad y fiabilidad de los resultados de la encuesta es mayor para el caso de los que no han comprado respecto a los que sí han comprado. Entre las razones para comprar destacan la comodidad, el precio y, por lo general, la experiencia de los usuarios ha sido satisfactoria pues el 97,9 por 100 de los usuarios que han hecho compras por Internet ha declarado que dicha compra ha cubierto sus expectativas «siempre» o «casi siempre».

* Director. Consejo Superior de Cámaras de Comercio, Industria y Navegación de España.

Sin embargo, al preguntar a quienes no han comprado por Internet las razones para no hacerlo, encontramos destacadamente varias razones relacionadas con la confianza (ver Gráfico 1): «Miedo a dar los datos personales», «desconfianza en el sistema de pago», «inseguridad/desconfianza», «desconfianza en la presentación del producto», «falta de información», «desconfianza en las tiendas existentes».

Aunque muchas veces este tipo de respuestas no son reflexivas y vienen inducidas por la tipificación de respuestas disponibles en la encuesta y por el estado de opinión al que contribuyen los medios de comunicación, no cabe duda que para muchas personas la presunción de que las condiciones asociadas a las compras por Internet no merecen confianza se ha instalado en su acervo cultural, de forma que difícilmente se replantearán si sus presunciones están justificadas.

2. ¿Es seguro el comercio electrónico?

Ésta es una de las preguntas de más actualidad para los empresarios y los consumidores. La respuesta nunca puede ser tajante en ningún sentido, pero en especial en su afirmación. Es un hecho que la seguridad total tiene un coste infinito y, por lo tanto, no es ni será nunca completamente seguro el comercio electrónico, de la misma forma que no lo es ningún tipo de comercio.

De todas formas sería bueno hacer un conjunto de reflexiones: ¿Es seguro volar?, la respuesta varía según a quién se le pregunte y, al final, se acaba respondiendo con expresiones o cifras comparativas: es la forma más segura de viajar, es la que tiene menor porcentaje de siniestralidad, etcétera, en el fondo se acaba recurriendo a la comparación.

Con el comercio electrónico ocurre lo mismo, y al final la pregunta debería ser: ¿es más inseguro el comercio electrónico que el comercio tradicional?

La repuesta tampoco es simple puesto que se compara un comercio con experiencia de siglos con uno de muy reciente creación pero, aún así, me gustaría hacer algunas preguntas que puedan generar reflexión: «Cuando una empresa pone una tienda ¿pone puertas para limitar su acceso?, ¿pone alarmas para evitar robos?, ¿tienen seguros para casos de siniestralidad?, etcétera», sin duda alguna las respuestas son en su mayoría afirmativas. ¿Se hace lo mismo cuando se pone una tienda o un negocio en la red?, la respuesta a dicha pregunta presenta sin duda muchos más interrogantes que en las anteriores.

Hoy en día se puede afirmar que existen los mecanismos y las herramientas para garantizar un alto nivel de seguridad en la red, mayor incluso que para el negocio tradicional. Existen aseguradoras que ofrecen seguros de responsabilidad civil, de robos, etcétera, existen los *firewalls* —equivalentes a los guardas de seguridad en la red los cuales permiten el acceso a ciertos usuarios y lo deniegan a otros— existen los certificados digitales —autenticas llaves de seguridad de las puertas virtuales de la tienda electrónica que a la vez permiten garantizar el no repudio de las transacciones— existen los antivirus, un sistema antivandalismo, etcétera.

En definitiva, el uso del comercio electrónico puede ser tan seguro como se desee, se planifique o se invierta en dicha seguridad de la misma forma que se haría en un negocio tradicional.

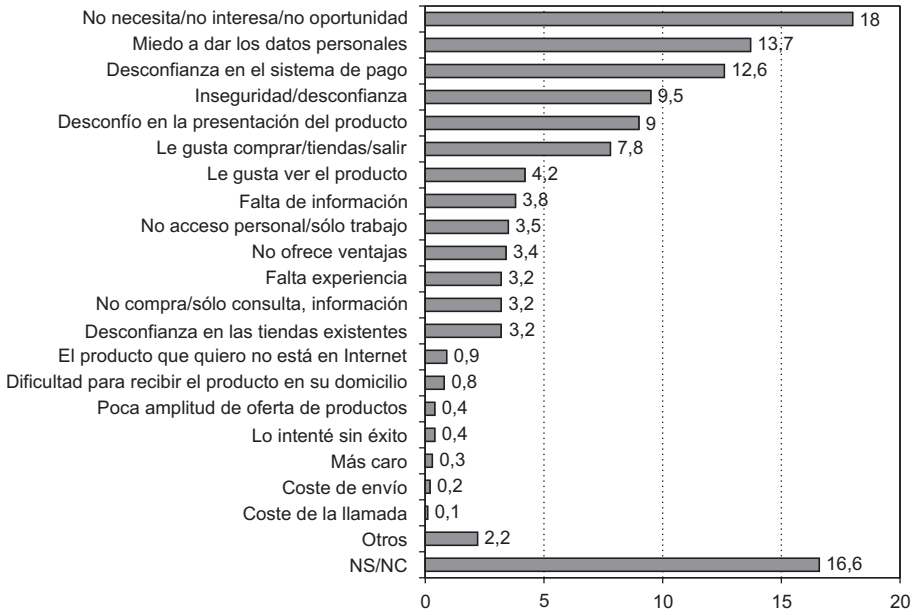
Pero, ¿cuál es la situación real o cómo se comportan las personas ante esta realidad? En este sentido, es llamativo que cuando las personas tienen que decidir sobre la adopción de medidas de seguridad en las empresas (y contribuir así a un clima más positivo en la percepción de los usuarios) aparentemente no son tan sensibles a las «malas noticias».

El estudio publicado por ASIMELEC en colaboración con el Ministerio de Ciencia y Tecnología en el marco del proyecto «Seguridad de la Información XXI» en el año 2003 [1] menciona un conjunto de estadísticas que deberían inquietar a las empresas:

- Los incidentes de seguridad se duplican cada año con respecto al anterior.
- Diariamente se descubren entre 2 y 5 nuevas vulnerabilidades.

GRÁFICO 1

RAZONES PARA NO COMPRAR POR INTERNET SEGÚN EL ESTUDIO DE AECE (En %)

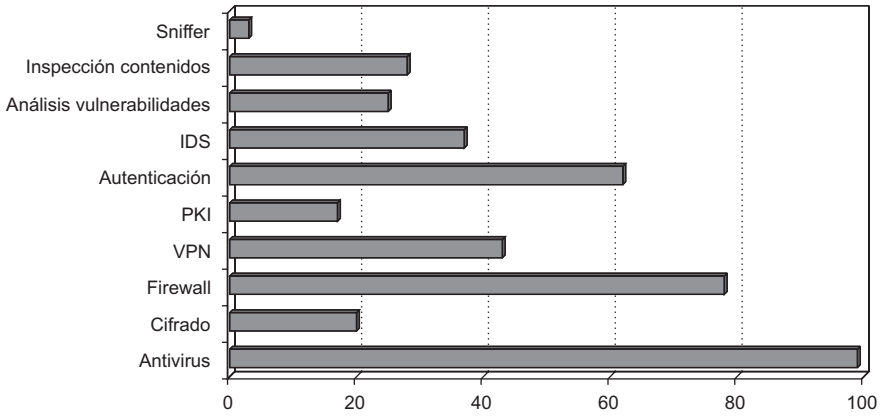


NOTA: Base 30,47 % de la muestra. Internautas no compradores.
FUENTE: AECE-fecemd.

- Los incidentes por virus provocaron pérdidas por 14.500 millones de euros en 2001.
- El 70 por 100 de las empresas medianas, el 84 por 100 de las grandes y el 89 por 100 de las muy grandes, han tenido pérdidas significativas por incidentes de seguridad en el año 2002.
- El gasto europeo en seguridad pasará de 2.000 millones de euros, en el año 2000, a alcanzar los 6.900 millones de euros, en 2005.
- El 54 por 100 de las empresas han incrementado su presupuesto para seguridad con respecto al año 2001, con un crecimiento medio del 25 por 100.
- Entre los años 2000 y 2001 la Agencia de Protección de Datos abrió expedientes sancionadores por 20 millones de euros.
- En el año 2001 la Agencia de Protección de Datos realizó 400 inspecciones.
- El 25 por 100 de las agencias del gobierno norteamericano son vulnerables a un ataque.
- Un 70 por 100 de 250 grandes empresas europeas no sabe cuándo ni con qué frecuencia revisa su política de seguridad.
- Más del 75 por 100 de las empresas españolas que basan su negocio en comercio electrónico a través de Internet vulneran en mayor o menor medida la LOPDCP.
- El estudio, realizado sobre 3.000 empresas de ámbito mundial, señala que los fallos de seguridad cuestan a las compañías entre el 5,7 y el 7 por 100 de sus ingresos anuales. Este concepto supuso unas pérdidas de 4.300 millones de dólares en empresas europeas.

GRÁFICO 2

MEDIDAS DE SEGURIDAD ADOPTADAS POR LAS EMPRESAS (En %)



FUENTE: ASIMELEC.

• Habiéndose multiplicado el número de ataques en la red por 2.400 en los últimos seis años produciendo unas perdidas valoradas en unos 250.000 millones de dólares, no se entiende que el presupuesto típico que una empresa de Internet destina a la seguridad sea menos del 5 por 100.

El marco del estudio de ASIMELEC pretende crear en las empresas un clima que promueva una actitud responsable ante la seguridad, por lo que incidir en los problemas detectados se considera un incentivo para la adopción de medidas.

En el citado estudio se comprueba el tipo de medidas de seguridad que adoptan las empresas en el ámbito de las tecnologías de la información (ver Gráfico 2).

No causa sorpresa el hecho de que las tecnologías más implantadas sean los antivirus y los *firewalls* (sistemas de protección perimetral de las comunicaciones), por el conocimiento de los problemas que se pueden afrontar con dichas soluciones y la relativa accesibilidad económica de la tecnología asociada.

En general las empresas no disponen de un tratamiento sistematizado de los retos de seguridad. Al preguntarles sobre las barreras existentes para la adopción de un enfoque metodológico como el que permite la adopción de las normas ISO/UNE 17799 y UNE 71501 y el Reglamento de Medidas de Seguridad RD994/1999, las conclusiones no pueden ser más reveladoras (ver Gráfico 3):

• El mayor obstáculo a la implantación de la seguridad es *la cultura empresarial,* por encima de los problemas que *a priori* podrían parecer más relevantes como presupuesto o tecnología.

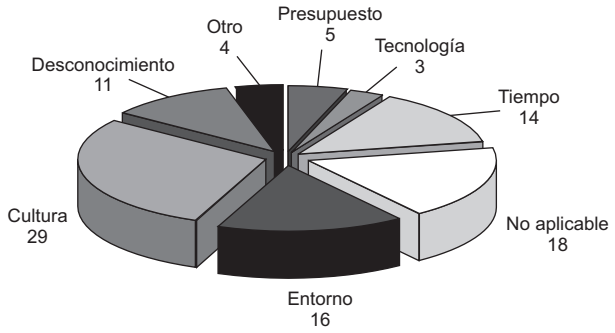
• Las organizaciones consideran que un porcentaje muy elevado de las recomendaciones de seguridad *no les son aplicables.* Únicamente entre un 5 por 100 y un 10 por 100 de las recomendaciones pueden no ser aplicables en función de la naturaleza de la organización, por lo que las respuestas de controles no aplicables realmente reflejan problemas de desconocimiento más que de no aplicabilidad.

• El nivel de *desconocimiento* de los distintos aspectos que condicionan la seguridad es también más alto de lo que cabía esperar.

La «cultura de la seguridad» estudiada, pues, bajo los prismas del usuario y de las empresas, revela sobre todo un alto grado de desconocimiento.

GRÁFICO 3

RAZONES QUE DIFICULTAN LA ADOPCIÓN DE METODOLOGÍAS SEGURAS EN LA EMPRESA (En %)



FUENTE: ASIMELEC.

Una de las formas de explicar el porqué de esta poca cultura de la seguridad en Internet podría ser el factor «histórico» del uso de Internet en la empresa. Si nos remontamos a hace siete u ocho años, el inicio de la popularización de Internet, es fácil recordar lo que ofrecían las empresas suministradoras de servicios Internet: conexión, correo electrónico y páginas *web*.

Si bien es cierto tanto lo primero como lo segundo, la evolución ha sido muy pequeña: los conceptos son los mismos, se ha mejorado en calidad, velocidad y precio, no ha ocurrido así con las páginas *web*.

En aquellos tiempos se ofrecía a la empresa la oportunidad de estar presente en Internet, se ofrecía el diseño de unas páginas y el *hosting* de éstas en los servidores. En el fondo se estaba ofreciendo la publicación de unos folletos de la empresa en un nuevo medio. Las reflexiones sobre la seguridad para las páginas *web* en aquellos tiempos eran inexistentes e innecesarias. ¿Qué nivel de seguridad tienen los folletos en papel? Ninguna. ¿Qué nivel de seguridad deberían tener los folletos digitales? Seguramente que algo más, pero realmente no era necesaria y los costes de ésta eran importantes.

Por lo tanto, se parte de un inicio donde la seguridad en la red, en el «comercio electrónico» no era un elemento importante.

A partir de esta primera fase, las empresas empezaron a sofisticar sus *web,* iniciaron el comercio electrónico más o menos interactivo. Se pasó de la simple publicación de folletos electrónicos a unos sistemas más sofisticados, donde el posible cliente podía ponerse en contacto con la empresa para hacer ciertos pedidos. Éstos en muchos casos eran formularios o bien correos electrónicos. En aquellos momentos tampoco se dio mucha importancia a la seguridad por dos motivos: primero, el volumen de transacciones era bajo y, en segundo lugar, se asimilaba la forma de realizar estas transacciones a la compra por teléfono. Y para la compra por teléfono, ¿qué niveles de seguridad se pedían?, realmente pocos.

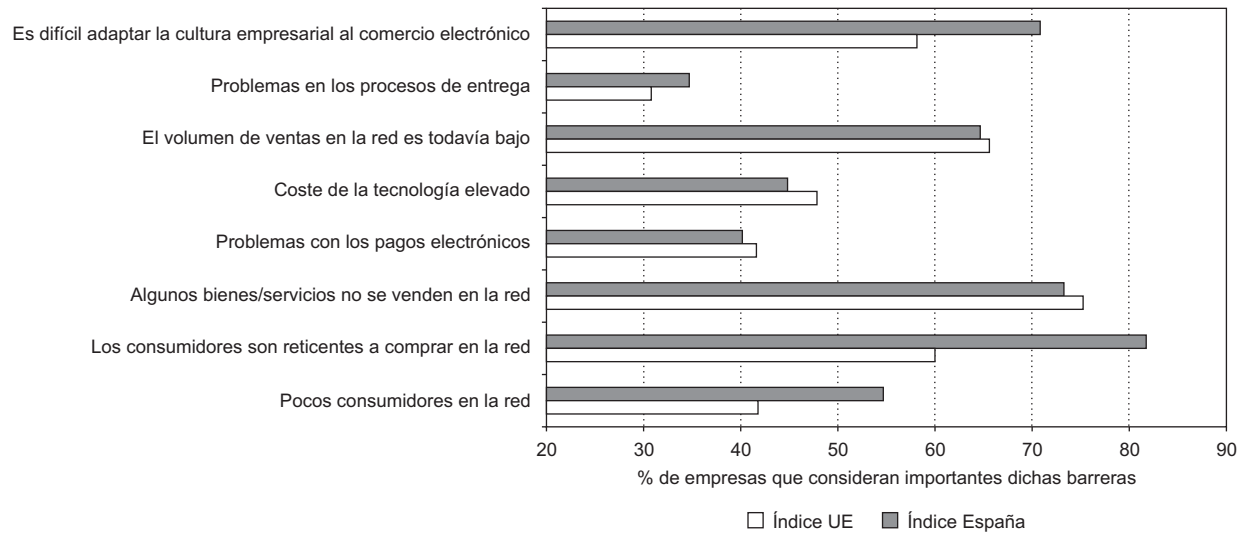
Durante la que podríamos llamar tercera fase, las empresas empezaron a automatizar los procesos de pedidos y de pagos. Aquí el tema de seguridad ya era importante por dos motivos: primero era necesario conectar las páginas *web* a los sistemas de gestión de las empresas, y por lo tanto era básico poder garantizar la confidencialidad de la información y poner barreras a los posibles intrusos. En segundo lugar era importante poder garantizar la identidad de quien compraba, puesto que el sistema de pago iba asociado a la transacción.

Pero ¿qué ocurría?, se partía ya de entornos desarrollados y en explotación. Se modificaban estos y se debía incorporar la seguridad a ellos. Esto hizo que en muchos casos, por cuestión de costes, no se implementaran todas las medidas de seguridad necesarias.

Y al final ¿qué tenemos?, pues un conjunto de comercios con unos niveles de seguridad no óptimos, y nos quejamos de la seguridad en la red. A nadie se le ocurriría abrir una tienda sin las mínimas medidas de seguridad, a nadie se le ocurriría crear una empresa sin alarmas, sin seguro, etcétera. Pero estas mismas personas y empresas, debido a las razones «históricas» antes mencionadas tienen empresas y tiendas sin el nivel de seguridad adecuado.

GRÁFICO 4

BARRERAS PARA LA VENTA ELECTRÓNICA
(En %)



FUENTE: Cámaras de comercio.

La tecnología existe, los costes de aplicar estos sistemas de seguridad son, en la mayoría de los casos, muy inferiores a los costes de implementar las mismas medidas en una tienda o empresa física.

No parece ser el caso español —un caso aislado en el marco europeo— aunque sí puede deducirse que en entornos tecnológicamente más avanzados o con grados de adopción de las tecnologías Internet más maduros, la resistencia de los compradores por la sensación de inseguridad disminuye.

Según un estudio elaborado por las cámaras de comercio [2] a partir de datos de la Comisión Europea, y analizando diversos sectores desde la perspectiva de ocho grandes líneas argumentales, se comprueba una cierta correlación en los resultados entre los aplicables a España y los aplicables al conjunto de Europa (ver Gráfico 4).

Para el conjunto de los sectores, de todos los obstáculos analizados, al que conceden mayor importancia los empresarios españoles es a la reticencia de los consumidores a realizar compras electrónicas, mientras que para los empresarios europeos la barrera más importante es que algunos bienes y servicios no se venden electrónicamente.

Tanto para los empresarios españoles como para los empresarios europeos, las trabas que dificultan menos las ventas electrónicas son los problemas que pueden generarse en los procesos de entrega y de pago electrónico.

Por todo lo dicho, puede concluirse que los usuarios españoles desconfían de las posibilidades transaccionales de Internet, y esta desconfianza es percibida también por los empresarios que se enfrentan a ésta como una más de las muchas dificultades que conlleva sacar adelante un negocio en el que la vertiente electrónica sea relevante.

Qué necesita una empresa para hacer comercio electrónico seguro en la red: garantizar la identidad, integridad, confidencialidad y no repudio de las transacciones

Internet, en tanto que red abierta, permite una comunicación interactiva entre los diferentes agentes que posiblemente no habían tenido ninguna relación anteriormente. Estas redes están siendo utilizadas por empresas que quieren sacar partido de la apertura de la red, la disminución de los costes, los entornos de trabajo compartido, el acceso a nuevos mercados, etcétera. Pero para lograr con éxito todos estos propósitos el entorno Internet tiene que ser seguro.

Desde el inicio de los negocios, y más concretamente de las transacciones comerciales, ha existido la preocupación del conocimiento que uno de los agentes podía tener sobre el otro antes de realizar un negocio. Siempre han existido dudas sobre la identidad de la empresa, su solvencia, etcétera. Toda esta situación se ha ido solucionando mediante diferentes medios tales como los registros de las sociedades, los certificados de origen, los informes comerciales, etcétera.

Pero desde la introducción del comercio y de los negocios dentro del mundo de las telecomunicaciones, y especialmente dentro de Internet, ha vuelto a tomar protagonismo esta problemática, puesto que en el mundo virtual muchas de las soluciones planteadas en el mundo real no tienen sentido o bien hay que implementar nuevas funciones intrínsecas del mundo de las telecomunicaciones.

Autenticación del emisor

Es necesario autentificar que quien realmente está enviando un mensaje, una factura, una cuenta bancaria, etcétera, es realmente quien dice que es. Esto en el mundo real no es tan complicado ya que con la presentación de unos poderes, con la firma manuscrita, la presencia física, etcétera, se soluciona la cuestión.

Seguridad de que la información transmitida sólo pueda ser leída, escuchada, alterada, etcétera, por el receptor

Éste es el segundo problema que se encuentra en el mundo virtual. Aquí puede haber escuchas e interferencias en el envío de la información que pongan en duda el negocio realizado.

Autenticación del receptor

Al igual que con el emisor hay que autentificar que quien está recibiendo el mensaje es quien realmente ha de ser y no hay suplantación de identidad con objetivos tan diversos como la obtención de información confidencial, la realización de transferencias bancarias, etcétera.

Garantía de no repudio de las operaciones (irrevocabilidad)

Hay ciertas operaciones en las que es necesario que tanto el receptor como el emisor tengan constancia de que la operación se ha realizado, y que esta constancia tenga validez ante un tercero.

Un individuo, cuando entra en Internet, puede navegar por diferentes servicios puestos en la red por terceras organizaciones, sin que estos organismos sepan quien está accediendo a sus páginas. Desaparece su identidad física para pasar a ser un ente invisible que puede «fisgar» por todas partes sin ser visto.

En el supuesto de que una persona quiera comprar algunos productos en una denominada «tienda virtual», un lugar o *web* en Internet donde se ofrecen productos y se pueden comprar mediante solicitud por la misma red, el problema que se plantea es el siguiente: ¿quién es el que pide este producto y dice que paga con un número de tarjeta de crédito?, ¿es quien dice ser o se trata de una suplantación o falsificación de identidad? Se ha de tener en cuenta que un cargo en una tarjeta sin la firma del propietario crea una inseguridad en muchos casos insostenible para el vendedor, ya que el importe puede ser devuelto a requerimiento del propietario hasta 6 meses después sin ningún tipo de impedimento.

Por otra parte está el tema de la transmisión de mensajes con seguridad, tanto de la identidad del emisor y del receptor, como del contenido del mensaje. Es relativamente fácil «pinchar» líneas de comunicación y «escuchar» los mensajes que se envían, alterar su contenido, o emular cuentas de correo electrónico de otras personas o entidades (enviar correo engañando al receptor sobre la identidad del emisor).

Y, por último, tenemos el problema del que vende el producto, ¿realmente es quien dice que es o es alguien que intenta conseguir números de visas para poderlos utilizar posteriormente como comprador en otras tiendas?

3. El certificado digital

Desde diferentes organismos internacionales se ha estado trabajando para solucionar estos problemas y se ha definido lo que debería ser la «identidad digital», que no es más que un sistema de seguridad por certificados, algo así como un DNI digital, es decir un identificador único dentro de la red que permita a su poseedor ser identificado como tal dentro de la misma con el fin de realizar un conjunto de acciones determinadas (firmar un documento, entrar en lugares restringidos, identificarse ante una administración, etcétera).

Los certificados son una herramienta imprescindible para garantizar la autenticidad del emisor y del receptor así como la integridad de la información transmitida, por tanto, hay que certificar a las empresas y a los servidores de comercio electrónico. Esto implica tener directorios de claves públicas, listas de revocación, sellos de tiempo y reglas operativas. Esto significa que existe una complejidad técnica y unos requisitos de seguridad que cualquier servidor de certificados debería cumplir. En este sentido, la Comisión Europea ha emitido una normativa específica que regula las entidades emisoras de certificados, especialmente en todos aquellos aspectos relacionados con dar las garantías necesarias a los usuarios de estos certificados a la hora de utilizarlos: seguridad, fiabilidad, estandarización, etcétera.

Uno de los aspectos más importantes dentro de este tipo de identidad digital es la entidad que emite este certificado, es decir, una vez que una empresa se identifica dentro de la red con un certificado digital, las otras partes tienen la seguridad de que esta empresa es realmente quien dice ser pues hay una tercera parte de confianza (la entidad emisora del certificado) que es quien da fe (certifica) de que es realmente quien dice ser. Por lo tanto, aunque en Internet podemos encontrar documentos firmados con certificados digitales, la validez de esta firma dependerá de quien ha emitido realmente el certificado, o dicho de otro modo, ¿tiene nuestra confianza el emisor del certificado a fin de identificar a la segunda parte? Un ejemplo en el mundo real sería comparar un documento identificativo como podría ser un DNI emitido por el Ministerio del Interior con un carnet de socio de un determinado club. Evidentemente los dos documentos identifican a una persona, pero uno tendrá una validez diferente a la del otro y, sin duda, el primero tendrá un mayor reconocimiento ante un desconocido que el segundo, aunque solamente con el segundo se pueda acceder a las instalaciones del club.

Existen ya diversas entidades que han empezado a emitir algún tipo de certificado. Se basan en pedir un informe de la existencia de la entidad que solicita la identidad, y le dan su clave privada. La cuestión es la aceptación del sistema de manera global, ya que no existe un estándar consensuado entre las diversas empresas que realizan el servicio y algunas pueden tener problemas de credibilidad por los escasos requisitos que solicitan, por el poco prestigio que puedan tener fuera de su demarcación territorial, etcétera.

4. Hacia la confianza internacional

Las cámaras de comercio son sensibles a las barreras que tienen que gestionar las empresas y desde hace varios años desarrollan a nivel internacional diversas iniciativas que contribuyen a que disminuyan esas cargas.

En este sentido, dos iniciativas relevantes son ChamberTrust y ChamberSign.

FIGURA 1

SELLO CHAMBERTRUST

FIGURA 2

INICIATIVA CHAMBERSIGN

ChamberTrust

El sello de confianza ChamberTrust (ver Figura 1) se otorga a las empresas a través de la Cámara de Comercio a la que pertenecen y permite su inclusión en un directorio mundial que incorpora ciertos datos de la empresa para promover la confianza en su relación con otras empresas a nivel internacional.

El sello Chambertrust está auspiciado por la Federación Mundial de Cámaras (WCF). La Federación Mundial de Cámaras (WCF) es la división especializada de la CCI (Cámara de Comercio Internacional) para sus cámaras de comercio miembros en todo el mundo. La WCF era anteriormente conocida como la Oficina Internacional de Cámaras de Comercio (IBCC).

A través de su red global de apoyo, la WCF permite a las Cámaras de todo el mundo intercambiar experiencias y mejorar su desempeño en áreas como finanzas, dirección y desarrollo y promoción de servicios.

La WCF trabaja estrechamente con organizaciones multilaterales de apoyo, como el Grupo del Banco Mundial y el Programa de las Naciones Unidas para el Desarrollo (PNUD), en proyectos de desarrollo de capacidad.

Todas las Cámaras que son miembros de la CCI son automáticamente miembros de la WCF. En la actualidad, Cámaras de más de 140 países son miembros de la CCI.

La institución cameral, con más de 400 años promoviendo la confianza a nivel internacional, está especialmente cualificada para promover iniciativas como el sello ChamberTrust.

A modo de herramienta de marketing, el principal objetivo de ChamberTrust es ayudar a seleccionar socios, compradores y/o proveedores verificando para ello la existencia real de la compañía, sus actividades y sus productos, así como el propietario real del sitio *web*.

Con un motor de búsqueda y un portal, ayuda a las empresas a atraer socios de negocios potenciales mediante bases de datos internacionales que incluyen la posibilidad de realizar búsquedas por actividad y por productos declarados por estas empresas.

Gracias a la imagen neutral e independiente de las cámaras de comercio, Industria y Navegación esta herramienta ofrece mayores y mejores oportunidades de contacto al incrementar el impacto y la visibilidad de las empresas en la red. De esta forma, ChamberTrust ayuda a las compañías a destacar entre la competencia y a ser seleccionadas por posibles socios de negocios.

ChamberSign

En 1999, Eurochambres y diez de sus organizaciones camerales de Alemania, Bélgica, Francia, España, Holanda, Italia, Luxemburgo, Reino Unido y Suecia esta-

blecieron la organización internacional ChamberSign (ver Figura 2), cuyo objetivo primordial consistía en proporcionar la interoperabilidad de las firmas electrónicas utilizadas por las empresas europeas (certificadas por las cámaras de comercio) para promover las relaciones empresariales transfronterizas que hicieran uso del comercio electrónico.

Las organizaciones camerales involucradas representan 579 cámaras de comercio próximas a las empresas, con una cobertura de más de 13 millones de tales empresas, muchas de las cuales son PYMES. El sistema pretende atraer otras organizaciones camerales de todo el mundo, de forma que se refuerce el concepto de red global cameral de firma electrónica.

Las cámaras de comercio han sido las primeras instituciones en adoptar e impulsar los estándares europeos que permiten, al amparo de la Directiva 1999/93/CE del Parlamento Europeo y el Consejo del 13 de diciembre por la que se establece un marco comunitario para la firma electrónica [3], expedir Certificados Reconocidos (nombre de la versión española de la Directiva del término *Qualified Certificates* que hubiera sido mejor traducir por «Certificados Cualificados» ya que el término adoptado introduce confusión al haber sido utilizado también en las normas españolas, y sólo en ellas).

La gestión de este tipo de certificados por las Cámaras uniformiza a nivel europeo el esquema de presunciones por el que se establece la equivalencia funcional entre la firma electrónica y la firma manuscrita.

5. La confianza en España

En esta misma línea, y con el objetivo de hacer Internet y el Comercio Electrónico más seguro, las cámaras de comercio pusieron en marcha, en julio de 2000, una iniciativa para garantizar la identidad de las empresas españolas que realicen Comercio Electrónico. Dicha iniciativa se estructuró en forma de sociedad anónima: AC Camerfirma S.A. es la primera CA que establece su prioridad en la emisión de certificados personales que señalan la relación entre una persona y una empresa, bien como empleado, bien como apoderado. A lo largo de su actividad establece la red de entidades de inscripción (RA) más tupida de España al contar con 45 cámaras de comercio (de un total de 85) capaces de desempeñar los trabajos de verificación de identidad asociados a dicha función.

En junio de 2001 comienza sus actividades Firmaprofesional, participada por AC Camerfirma y los Colegios Oficiales de Médicos, Farmacéuticos y Arquitectos de Cataluña. Su vocación es la de desarrollar los servicios de certificación de todos los Colegios Profesionales, atendiendo a la potestad que sólo estos tienen de acreditar quién es colegiado, tras verificar que se cumplen los requisitos para ello. Es un modelo que busca optimizar el esquema de costes a base de replicar en diferentes colegios el exigente entorno técnico y operativo capaz de satisfacer todos los requisitos legales, y conociendo en profundidad sus necesidades.

6. Contexto legal de la certificación en España

El desarrollo de los mecanismos de confianza en torno a la certificación ha atravesado una etapa compleja y de escaso valor, que ha requerido de un gran esfuerzo por parte de las cámaras de comercio.

El Real Decreto-Ley 14/1999, de 17 de septiembre, por el cual se regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación, y la Orden de 21 de febrero de 2000 por la que se aprueba el Reglamento de acreditación de prestadores de servicios de certificación y de certificación de determinados productos de firma electrónica, han sido instrumentos de escaso valor que ha sido preciso interpretar a la luz de la Directiva 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de diciembre de 1999, por la que se establece un marco comunitario para la firma electrónica. Es decir, hasta la reciente publicación de la Ley 59/2003, de 19 de diciembre, de firma electrónica [5], ha tenido más valor para la actividad de los prestadores de servicios de

certificación la Directiva, que la ley y el reglamento que la transponían.

Entre los motivos que condujeron a ello cabe citar las contradicciones respecto a la Directiva y la falta de desarrollo de los medios para poder cumplir los requisitos que se establecían, ya que no era posible inscribir al prestador de servicios de certificación en un registro que no se llegó a crear, ni evaluar a los prestadores de servicios de certificación, puesto que no existía ni la normativa de evaluación ni las entidades evaluadoras.

A partir de esta situación legal de partida tan dificultosa para la prestación de servicios de certificación digital en el ámbito privado, la Orden del Ministerio de Hacienda HAC/1181/2003, de 12 de mayo, y la reciente Ley 59/2003, de 19 de diciembre, de firma electrónica, han venido a impulsar el sector de la certificación.

Efectivamente, la nueva ley determina que será el Ministerio de Ciencia y Tecnología el que establecerá el reconocimiento de los prestadores de servicios de certificación y dará por finalizado un período en el que se ha producido una amplia normativa de menor rango con criterios muy diversos en lo que se refiere a dicho reconocimiento.

La nueva situación legal dará las mismas oportunidades a los distintos proveedores de certificación digital, y permitirá el desarrollo de otros prestadores alternativos.

7. Usos de los certificados para firma electrónica

La seguridad de las transacciones se consigue a través de mecanismos que favorecen la confidencialidad de las comunicaciones o la autenticación de los intervinientes.

Para ello, los extremos de la comunicación tienen que estar dotados de los mecanismos técnicos que posibiliten el uso de la criptografía y de los certificados.

La panoplia de servicios posibles es extensa, éstos son algunos de los usos:

Cifrado

Los sistemas de clave pública permiten el cifrado de los datos utilizando la clave pública del destinario. De esta forma, únicamente el destinatario —poseedor de la clave privada— podrá acceder a la información.

Firma en algunas aplicaciones de amplio uso

El impulso de la firma electrónica en los últimos años ha motivado que las principales empresas de desarrollo de *software* hayan adaptado sus aplicaciones a las tecnologías de PKI. Entre estas aplicaciones debemos destacar la posibilidad de firmar disponibles en las aplicaciones que integran el Office XP y la solución de Adobe para la firma de PDF con el Acrobat.

Factura telemática

El impulso definitivo de la facturación telemática viene de la mano de la Orden HAC/3134/2002 y en especial de la reciente Resolución 2/2003, de 14 de febrero, del Director General de la Agencia Estatal de Administración Tributaria.

Relaciones con la Agencia Tributaria

Es sin duda en el ámbito Tributario donde se han conseguido los mayores avances en la denominada Administración *on-line,* e-Administración o e-Goverment, pudiendo realizarse en la actualidad un gran número de actos con la AEAT, entre los que destacan especialmente los relativos a la presentación de declaraciones de carácter tributario y, entre ellos los referentes a los tributos del IRPF, IVA, Sociedades, Patrimonio, Aduanas e Impuestos Especiales.

Partes de accidentes de trabajo

El proyecto Delt@ es una iniciativa del Ministerio de Trabajo para facilitar la presentación de los partes de baja laboral por medios telemáticos.

Toma de decisiones en juntas universales

La reciente Ley 26/2003, de 17 julio, por la que se modifican la Ley 24/1988, de 28 de julio de 1988, del Mercado de Valores, y el texto refundido de la Ley de Socie-

dades Anónimas, aprobado por el Real Decreto Legislativo 1564/1989, de 22 de diciembre de 1989, con el fin de reforzar la transparencia de las sociedades anónimas cotizadas define y promueve la posibilidad de que los accionistas puedan votar de forma electrónica en las Juntas. Ésta es sólo una de las posibilidades de votación, que pueden extenderse a todo tipo de procesos electorales o referéndums que podrán ser realizados de manera rápida y segura y de forma *on line* mediante la utilización de certificados digitales.

Contratación telemática

La aún reciente Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico, regula en el título IV la contratación por vía electrónica. La aportación de una prueba cualificada de la celebración de los contratos electrónicos se configura como un elemento fundamental en este tipo de relaciones, por lo que la utilización de la firma electrónica en general y de los certificados Camerfirma en especial, se perfila como un elemento prácticamente indispensable a la hora de contratar por estos medios.

Servicios que requieren control de identidad en el *e-Commerce*

Todos los servicios ofrecidos de forma *on line* y que requieran una correcta identificación del usuario podrán beneficiarse de la firma electrónica y de los certificados digitales. Mediante la utilización de certificados digitales, cuando un usuario accede por ejemplo a un *Market Place,* el sistema podrá controlar y limitar su forma de acceso en función de la persona que se lo presente, pudiendo además firmar los pedidos que realice a modo de prueba de compra y contratación electrónica.

Además de los usos anteriormente citados, se pueden señalar también los siguientes: firma de escritorio, seguridad del correo electrónico, SSL, control de acceso en las *web* e intranet, cumplimiento de niveles altos LOPD con SSL, *e-Commerce* financiero, etcétera.

8. Conclusiones

Las estadísticas muestran como común denominador el desconocimiento de los usuarios cuando desconfían de Internet como plataforma de realización de transacciones y el de las empresas cuando no son conscientes de las ventajas que tiene la adopción de medidas de seguridad o lo catastrófico que puede ser no contar con ellas.

Las cámaras de comercio, teniendo en cuenta las tecnologías existentes, promueven soluciones técnicas para reforzar la seguridad de las transacciones y desarrollan un gran esfuerzo de difusión y formación entre las empresas.

Todo ello orientado hacia un objetivo de competitividad de las empresas y ciudadanos españoles en un complejo mundo virtual en el que no es asumible ningún retraso en relación con los países de nuestro entorno.

Referencias bibliográficas

[1] ASIMELEC (2003): Estudio sobre el estado actual de la seguridad de los sistemas de la información en las empresas entrevistadas, de acuerdo con la Norma ISO/IEC17799: 2000.

[2] CÁMARAS DE COMERCIO (2003): Estudio sobre las Barreras Sectoriales para la Venta Electrónica.

[3] DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 13 de diciembre de 1999 por la que se establece un marco comunitario para la firma electrónica, Diario Oficial de las Comunidades Europeas, 19-1-2000.

[4] ESTUDIO COMERCIO ELECTRÓNICO B2C EN ESPAÑA, VENTAS AL CONSUMIDOR-B2C, AECE-fecemd 2003.

[5] LEY 59/2003, de 19 de diciembre, de firma electrónica, BOE de 20 de diciembre de 2003.